ABSTRACT

"A Method of Exchanging Digital Data"

A method of exchanging digital signatures (sign_A, sign_B) between a first and a second party (A,B) includes the first party (A) encrypting their signature (sign_A) and generating an authentication certificate (Cert_A), the authentication certificate (Cert_A) authenticating that the encrypted signature (C_T) is an encryption of the signature (sign_A). The first party (A) sends the encrypted signature (C_T) and the authentication certificate (Cert_A) to the second party (B). The second party (B) verifies that the encrypted signature (C_T) is an encryption of the digital signature (sign_A) of the first party (A), and if the verification is positive, the second party (B) sends its digital signature (sign_B) to the first party (A). The first party (A) verifies that the digital signature (sign_B) is the digital signature of the second party (B), and if the verification is positive the first party sends its unencrypted signature (sign_A) to the second party (B). The second party (B) verifies that the digital signature (sign_A) is the first party's digital signature, and accepts the digital signature (sign_A) if the verification is positive. If the verification is negative, the second party (B) sends the encryted digital signature (C_T) and its digital signature (sign_B) to a third party (T). The third party (T) is independent of the first and second parties (A,B) and has a decryption key to decrypt the encrypted digital signature (C_T) of the first party (A).

The third party (T) decrypts the encrypted digital signature (C_T) to obtain the first party's digital signature (sign_A), and verifies that the digital signatures (sign_A, sign_B) are the digital signatures of the first and second party (A,B) respectively. If both digital signatures (sign_A, sign_B) are verified as the digital signatures of the first and second parties (A,B), the third party (T) sends the first party's digital signature (sign_A) to the second party (B) and sends the second party's digital signature (sign_B) to the first party (A).

Figure 1